WHAT IS CLAIMED IS:

1. An apparatus for authenticating a digital signature, comprising:

a signature generating part encrypting a digital document by using a private key defined by a signer and digest information for checking whether the digital document has been tampered with, and generating a digital signature;

a signature synthesizing part creating image information by synthesizing the digital signature and a predetermined mark; and

an image embedding part embedding the image information created by said signature synthesizing part into an indicated position in the digital document.

2. The apparatus as claimed in claim 1, wherein said signature synthesizing part comprises an image information generating part generating pixel data for the image information including the digital signature,

wherein:

a palette, where first color information is defined for first index information and second color information is defined for other index information, is referred to;

the first index information is defined for pixels used for the predetermined mark; and

each of the other index information, which corresponds to each number of a number string forming

the digital signature, is defined for each of other pixels.

3. The apparatus as claimed in claim 2, wherein said image information generating part assigns each of the other indication information corresponding to each number of the number string to each pixel from a beginning of the number string forming the digital signature while skipping the pixels used for the predetermined mark.

4. An apparatus for authenticating a digital signature, comprising:

a signature extracting part extracting the digital signature from image information embedded into a digital document;

a digest obtaining part decrypting the digital signature by a public key opened by a signer and obtaining first digest information for checking whether the digital document has been tampered with; and

an authenticating part determining whether second digest information regenerated based on the digital document identically corresponds to the first digest information obtained by said digest obtaining part and authenticating the digital signature based on a result of the determination.

5. The apparatus as claimed in claim 5, wherein said signature extracting part refers to a palette where first color information is defined for first index information and second color information is defined for other index information, and defines partial pixel data, formed by removing the first index information from pixel data forming the image information, as the digital signature, so as to generate the digital signature.

6. A method for authenticating a digital signature, comprising the steps of:

(a) encrypting a digital document by using a private key defined by a signer and digest information for checking whether the digital document has been tampered with, and generating a digital signature;

(b) creating image information by synthesizing the digital signature and a predetermined mark; and

(c) embedding the image information created in said step (b) into an indicated position in the digital document.

7. A method for authenticating a digital signature, comprising the steps of:

(a) extracting the digital signature from image information embedded into a digital document;

(b) decrypting the digital signature by a public key opened by a signer and obtaining first digest information for checking whether the digital

document has been tampered with; and

(c) determining whether second digest information regenerated based on the digital document identically corresponds to the first digest information obtained by said step (b) and authenticating the digital signature based on a result of the determination.

8. A computer-readable recording medium having a program recorded therein for causing a computer to authenticate a digital signature, said program comprising the codes of:

(a) encrypting a digital document by using a private key defined by a signer and digest information for checking whether the digital document has been tampered with, and generating a digital signature;

(b) creating image information by synthesizing the digital signature and a predetermined mark; and

(c) embedding the image information created in said step (b) into an indicated position in the digital document.

9. The computer-readable recording medium as claimed in claim 8, wherein said code (b) includes a code of (d) generating pixel data for the image information including the digital signature,

wherein:

a palette, where first color information is defined for first index information and second

color information is defined for other index information, is referred to;

the first index information is defined for pixels used for the predetermined mark; and

each of the other index information, which corresponds to each number of a number string forming the digital signature, is defined for each of other pixels.

10. The computer-readable recording medium as claimed in claim 9, wherein said code (d) assigns each of the other indication information corresponding to each number of the number string to each pixel from a beginning of the number string forming the digital signature while skipping the pixels used for the predetermined mark.

11. A computer-readable recording medium having a program recorded therein for causing a computer to authenticate a digital signature, said program comprising the codes of:

(a) extracting the digital signature from image information embedded into a digital document;

(b) decrypting the digital signature by a public key opened by a signer and obtaining first digest information for checking whether the digital document has been tampered with; and

(c) determining whether second digest information regenerated based on the digital document identically corresponds to the first digest information obtained by said code (b) and

authenticating the digital signature based on a result of the determination.

12. The computer-readable recording medium as claimed in claim 11, wherein said signature extracting part refers to a palette where first color information is defined for first index information and second color information is defined for other index information, and defines partial pixel data, formed by removing the first index information from pixel data forming the image information, as the digital signature, so as to generate the digital signature.